2025 -- S 1037 SUBSTITUTE A AS AMENDED

========
LC002859/SUB A
========

S T A T E O F R H O D E I S L A N D

IN GENERAL ASSEMBLY

JANUARY SESSION, A.D. 2025

A N A C T

RELATING TO CRIMINAL OFFENSES -- IDENTITY THEFT PROTECTION ACT OF 2015

Introduced By: Senators Gu, Zurier, Burke, Ciccone, Urso, DiPalma, Vargas, Paolino, Tikoian, and Lawson
Date Introduced: May 09, 2025

Referred To: Senate Artificial Intelligence & Emerging Tech

It is enacted by the General Assembly as follows:

SECTION 1. Sections 11-49.3-2, 11-49.3-3, 11-49.3-4, 11-49.3-5, 11-49.3-6 and 11-49.3-7 of the General Laws in Chapter 11-49.3 entitled "Identity Theft Protection Act of 2015" are hereby amended to read as follows:

11-49.3-2. Risk-based information security program.

(a) A municipal agency, state agency, or person who or that stores, collects, processes, maintains, acquires, uses, owns, or licenses ~~personal~~ personally identifiable information about a Rhode Island resident shall, at a minimum, implement and maintain a risk-based information security program that meets current best practices of an approved and industry recognized cybersecurity framework that contains reasonable security procedures, programs and practices appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the ~~personal~~ personally identifiable information from unauthorized access, use, modification, destruction, or disclosure and to preserve the confidentiality, integrity, and availability of such information. Controls and procedures shall be implemented to restrict and manage access to the data in transit and at rest. A municipal agency, state agency, or person shall not retain ~~personal~~ personally identifiable information for a period longer than is reasonably required to provide the services requested; to meet the purpose for which it was collected; or in accordance with a written retention policy or as may be required by law. A municipal agency, state agency, or person shall destroy all ~~personal~~ personally identifiable information, regardless of the medium that such information is in, in a secure manner, including,

but not limited to, shredding, pulverization, incineration, or erasure in accordance with current best practices of an approved and industry recognized sanitization and destruction guideline.

(b) A municipal agency, state agency, or person who or that discloses ~~personal~~ personally identifiable information about a Rhode Island resident to a nonaffiliated third party shall require by written contract that the third party and any sub-contracted party implement and maintain reasonable security procedures, programs and practices that meet current best practices of an approved and industry recognized cybersecurity framework and are appropriate to the size and scope of the organization; the nature of the information; and the purpose for which the information was collected in order to protect the ~~personal~~ personally identifiable information from unauthorized access, use, modification, destruction, or disclosure. The provisions of this section shall apply to contracts entered into after the effective date of this act.

(c) Municipal and state agencies shall provide an annual update to the general assembly and the division of enterprise technology strategy and services (ETSS) or successor state agency, or successor to the chief digital officer in the form required by the ETSS.

11-49.3-3. Definitions.

(a) The following definitions apply to this chapter:

(1) "Breach of the security of the system" means unauthorized access or acquisition of ~~unencrypted,~~ computerized data information that compromises the security, confidentiality, or integrity of ~~personal~~ personally identifiable information maintained by the municipal agency, state agency, or person. Good-faith acquisition of ~~personal~~ personally identifiable information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system; provided, that the ~~personal~~ personally identifiable information is not used or subject to further unauthorized disclosure.

(2) ~~"Classified data" means any data that is not public (private, sensitive, confidential). Classified data requires additional security controls, such as access restrictions and encryption. Classified data includes personally identifiable information (PII), personally identifiable health information (PHI), or federal tax information (FTI).~~

~~(3)~~ "Cybersecurity incident" means unauthorized access that could jeopardize the confidentiality, integrity, or availability of critical information systems and critical infrastructure systems (i.e., first responder networks, water, energy).

~~(4)~~(3) "Encrypted" means the transformation of data through the use of a one hundred twenty-eight (128) bit or higher algorithmic process into a form in which there is a low probability of assigning meaning without use of a confidential process or key. Data shall not be considered to be encrypted if it is acquired in combination with any key, security code, or password that would

permit access to the encrypted data.

~~(5)~~(4) "Health insurance information" means an individual's health insurance policy number, subscriber identification number, or any unique identifier used by a health insurer to identify the individual.

~~(6)~~(5) "Medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a healthcare professional or provider.

~~(7)~~(6) "Municipal agency" means any department, division, agency, commission, board, office, bureau, authority, quasi-public authority, or school, fire, or water district within Rhode Island, other than a state agency, and any other agency that is in any branch of municipal government and exercises governmental functions other than in an advisory nature.

~~(8)~~(7) "Owner" means the original collector of the information.

~~(9)~~(8) "Person" shall include any individual, sole proprietorship, partnership, association, corporation, joint venture, business, legal entity, trust, estate, cooperative, or other commercial entity.

~~(10) "Personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when the name and the data elements are not encrypted or are in hard copy, paper format:~~

~~(i) Social security number;~~

~~(ii) Driver's license number, Rhode Island identification card number, or tribal identification number;~~

~~(iii) Account number, credit or debit card number, in combination with any required security code, access code, password, or personal identification number, that would permit access to an individual's financial account;~~

~~(iv) Medical or health insurance information; or~~

~~(v) E-mail address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.~~

(9) "Personally identifiable information" means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. This information includes both direct and indirect identifiers, as well as biometric data and internet data.

(10) "Reasonable security procedures" means protective, documented measures that are commensurate with the risk and sensitivity of the data, suitable for the specific context, including nature of the business and type of data; effective in preventing unauthorized access, use, disclosure,

alteration or destruction of the data. Reasonable security procedures are regularly reviewed and updated to ensure they remain effective and relevant in the face of evolving threats and include who is responsible for implementing and maintaining the procedures, how they are implemented and how they are regularly reviewed.

(11) "Remediation service provider" means any person who or that, in the usual course of business, provides services pertaining to a consumer credit report including, but not limited to, credit report monitoring and alerts, that are intended to mitigate the potential for identity theft.

(12) "State agency" means any department, division, agency, commission, board, office, bureau, authority, or quasi-public authority within Rhode Island; either branch of the Rhode Island general assembly or an agency or committee thereof; the judiciary; or any other agency that is in any branch of Rhode Island state government and that exercises governmental functions other than in an advisory nature.

(b) For purposes of this chapter, ~~personal~~ personally identifiable information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(c) For purposes of this chapter, "notice" may be provided by one of the following methods:

(1) Written notice;

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in 15 U.S.C. § 7001; or

(3) Substitute notice, if the municipal agency, state agency, or person demonstrates that the cost of providing notice would exceed twenty-five thousand dollars ($25,000), or that the affected class of subject persons to be notified exceeds fifty thousand (50,000), or the municipal agency, state agency, or person does not have sufficient contact information. Substitute notice shall consist of all of the following:

(i) E-mail notice when the municipal agency, state agency, or person has an e-mail address for the subject persons;

(ii) Conspicuous posting of the notice on the municipal agency's, state agency's, or person's website page, if the municipal agency, state agency, or person maintains one; and

(iii) Notification to major statewide media.

11-49.3-4. Notification of breach.

(a)(1) Any municipal agency, state agency, or person who or that stores, owns, collects, processes, maintains, acquires, uses, or licenses data that includes ~~personal~~ personally identifiable information shall provide notification as set forth in this section of any disclosure of ~~personal~~ personally identifiable information, or any breach of the security of the system, that poses a

significant risk of identity theft to any resident of Rhode Island whose ~~personal~~ personally identifiable information was, or is reasonably believed to have been, acquired by an unauthorized person or entity.

(2) The notification shall be made in the most expedient time possible, subject to the following:

(i) For state and municipal agencies, no later than thirty (30) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d), and shall be consistent with the legitimate needs of law enforcement as provided in subsection (b). In the event that more than five hundred (500) Rhode Island residents are to be notified, the municipal agency or state agency shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general, the division of enterprise technology strategy and services (ETSS) or successor state agency or successor to the chief digital officer and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents. Where affected employees are represented by a labor union through a collective bargaining agreement, the employer shall also notify the collective bargaining agent, or designee, of such breaches.

(ii) For persons subject to subsection (a)(1), which is not a state or municipal agency, no later than forty-five (45) calendar days after confirmation of the breach and the ability to ascertain the information required to fulfill the notice requirements contained in subsection (d), and shall be consistent with the legitimate needs of law enforcement as provided in subsection (b). In the event that more than five hundred (500) Rhode Island residents are to be notified, the person shall notify the attorney general and the major credit reporting agencies as to the timing, content, and distribution of the notices and the approximate number of affected individuals. Notification to the attorney general, the division of enterprise technology strategy and services (ETSS) or successor state agency or successor to the chief digital officer and the major credit reporting agencies shall be made without delaying notice to affected Rhode Island residents.

(b) The notification required by this section may be delayed if a federal, state, or local law enforcement agency determines that the notification will impede a criminal investigation. The federal, state, or local law enforcement agency must notify the municipal agency, state agency, or person of the request to delay notification without unreasonable delay. If notice is delayed due to such determination, then, as soon as the federal, state, or municipal law enforcement agency determines and informs the municipal agency, state agency, or person that notification no longer poses a risk of impeding an investigation, notice shall be provided as soon as practicable pursuant

to subsection (a)(2). The municipal agency, state agency, or person shall cooperate with federal, state, or municipal law enforcement in its investigation of any breach of security or unauthorized acquisition or use, which shall include the sharing of information relevant to the incident; provided however, that such disclosure shall not require the disclosure of confidential business information or trade secrets.

(c) Any municipal agency, state agency, or person required to make notification under this section and fails to do so is liable for a violation as set forth in § 11-49.3-5.

(d) The notification to individuals must include the following information to the extent known:

(1) A general and brief description of the incident, including how the security breach occurred and the number of affected individuals;

(2) The type of information that was subject to the breach;

(3) Date of breach, estimated date of breach, or the date range within which the breach occurred;

(4) Date that the breach was discovered;

(5) A clear and concise description of any remediation services offered to affected individuals including toll free numbers and websites to contact:

(i) The credit reporting agencies;

(ii) Remediation service providers;

(iii) The attorney general, the division of enterprise technology strategy and services (ETSS) or successor state agency or successor to the chief digital officer; and

(6) A clear and concise description of the consumer's ability to file or obtain a police report; how a consumer requests a security freeze and the necessary information to be provided when requesting the security freeze; and that fees may be required to be paid to the consumer reporting agencies.

(e) For state and municipal agencies remediation services to be provided and to be described pursuant to the provisions of subsection (d)(5) of this section shall include, but not be limited to:

(1) Individuals eighteen (18) years of age and older, a minimum of five (5) years of coverage; and

(2) Individuals under eighteen (18) years of age, coverage until age eighteen (18), and no less than two (2) years of coverage beyond age eighteen (18).

11-49.3-5. Penalties for violation.

(a) Each reckless violation of this chapter is a civil violation for which a penalty of not

more than one hundred dollars ($100) per record may be adjudged against a defendant.

(b) Each knowing and willful violation of this chapter is a civil violation for which a penalty of not more than two hundred dollars ($200) per record may be adjudged against a defendant.

(c) Whenever the attorney general has reason to believe that a violation of this chapter has occurred and that proceedings would be in the public interest, the attorney general may bring an action in the name of the state against the business or person in violation.

(d) In addition to the penalties listed in this section, courts may impose additional appropriate sanctions as warranted by the circumstances.

11-49.3-6. Agencies or persons with security breach procedures.

(a) Any municipal agency, state agency, or person shall be deemed to be in compliance with the security breach notification requirements of § 11-49.3-4 if:

(1) The municipal agency, state agency, or person maintains its own security breach procedures as part of an information security ~~policy~~ program that meets or exceeds the requirements of this chapter for the treatment of ~~personal~~ personally identifiable information and at a minimum, adheres to the timing and notification ~~otherwise complies with the timing~~ requirements of § 11-49.3-4~~, and notifies subject persons in accordance with such municipal agency's, state agency's, or person's notification policies in the event of a breach of security~~; or

(2) The person maintains a security breach procedure pursuant to the rules, regulations, procedures, or guidelines established by the ~~primary or~~ applicable federal functional regulator, as defined in 15 U.S.C. § 6809(2), and notifies subject persons in accordance with the policies or the rules, regulations, procedures, or guidelines established by the ~~primary or~~ applicable federal functional regulator in the event of a breach of security of the system.

(b) A financial institution, trust company, credit union, or its affiliates that is subject to and examined for, and found in compliance with, the Federal Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice shall be deemed in compliance with this chapter.

(c) A provider of health care, healthcare service plan, health insurer, or a covered entity governed by the medical privacy and security rules issued by the federal Department of Health and Human Services, Parts 160 and 164 of Title 45 of the Code of Federal Regulations, established pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) shall be deemed in compliance with this chapter.

11-49.3-7. Notification of cybersecurity incident.

(a) Any municipal agency or state agency that detects a cybersecurity incident shall provide notification to the Rhode Island state police upon detection of the cybersecurity incident within

twenty-four (24) hours. The state police shall notify the division of enterprise technology strategy and services (ETSS) or successor state agency or successor to the chief digital officer within twenty-four (24) hours, or the next business day, of initial notification.

(b) Any municipal agency or state agency required to make notification under this section and fails to do so may be liable for a violation as set forth in § 11-49.3-5.

(c) The notification shall include, at a minimum, the following information to the extent known:

(1) A general and brief description of the incident, including how the cybersecurity incident occurred; and

(2) The date of the cybersecurity incident, estimated date of the cybersecurity incident, or the date range within which the cybersecurity incident occurred.;

(3) Any mitigating actions taken; and

(4) Any notifications to regulatory or federal entities.

SECTION 2. This act shall take effect on July 1, 2025.

========
LC002859/SUB A
========

EXPLANATION

BY THE LEGISLATIVE COUNCIL

OF

A N A C T

RELATING TO CRIMINAL OFFENSES -- IDENTITY THEFT PROTECTION ACT OF 2015

***

This act would amend the Identity Theft Protection Act of 2015. The act would eliminate the definitions for "classified data" and "personal information" and establish a definition for "personally identifiable information". This act would also add division of enterprise technology strategy and services (ETSS) or successor state agency, or successor to the chief digital officer to notification requirement provisions of the chapter. This act would raise the penalty provisions for violations.

This act would take effect on July 1, 2025.

========
LC002859/SUB A
========